EPODOC / EPO

PN - JP11272616 A 19991008

PD - 1999-10-08

PR - JP19980072563 19980320

OPD - 1998-03-20

TI - DATA COMMUNICATION SYSTEM FOR EXECUTING DATA ACCESS CONTROL

IN - SAITO TOMOHIKO

PA - NRI & NCC CO LTD

IC - G06F15/00 ; G06F12/14 ; G06F13/00 ; G09C1/00 ; H04L9/32 ; H04L9/36

© WPI / DERWENT

TI - Data access control system of data communication system - adds data security information to data, based on degree of security level specified by application unit and stores it in memory

PR - JP19980072563 19980320

PN - JP11272616 A 19991008 DW199954 G06F15/00 009pp

PA - (NOMU-N) NOMURA SOGO KENKYUSHO KK

IC - G06F12/14 ;G06F13/00 ;G06F15/00 ;G09C1/00 ;H04L9/32 ;H04L9/36

AB - JP11272616 NOVELTY - The data access control system β) adds data security information to data, based on the degree of security level specified by application unit (AP) and stores it in memory. During data access, matching of stored data security information and received data security level is performed, based on which application unit is allowed to access data.

- USE - In data communication system.
- ADVANTAGE - Maintains secrecy of data, reliably. DESCRIPTION OF DRAWING(S) - The figure shows data communication system. (3) Data access control system; (AP) Application unit.
- (Dwg.1/3)

OPD - 1998-03-20

AN - 1999-623958 [54]

© PAJ / JPO

PN - JP11272616 A 19991008

PD - 1999-10-08

AP - JP19980072563 19980320

IN - SAITO TOMOHIKO

PA - NRI & NCC CO LTD

TI - DATA COMMUNICATION SYSTEM FOR EXECUTING DATA ACCESS CONTROL

AB - PROBLEM TO BE SOLVED: To obtain a system capable of surely maintaining the secrecy of data by a simple constitution by permitting data access in a case that the data security level of an application means which tried access is equal to or higher than the data security level of data which was tried to be accessed.

- SOLUTION: A server Sn receives data transferred by a server SI and stores it. An application means AP connected to this server Sn tries the access of data regularly or at the time of receiving information on the reception of data from a server. The server Sn receiving the access request of data from the means AP permits data access only when the group of the means AP which tried access and the group of data security information are equal to each other and the data security level of the means AP is equal to or higher than the data security level of data which was tried to be accessed.

I - G06F15/00 ;G06F12/14 ;G06F13/00 ;G09C1/00 ;H04L9/32 ;H04L9/36

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－272616

(43)公開日　平成11年(1999)10月８日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｄ
	12/14	３１０		12/14	３１０Ｋ
	13/00	３５１		13/00	３５１Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｅ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７１

審査請求　未請求　請求項の数３　ＯＬ　（全９頁）　最終頁に続く

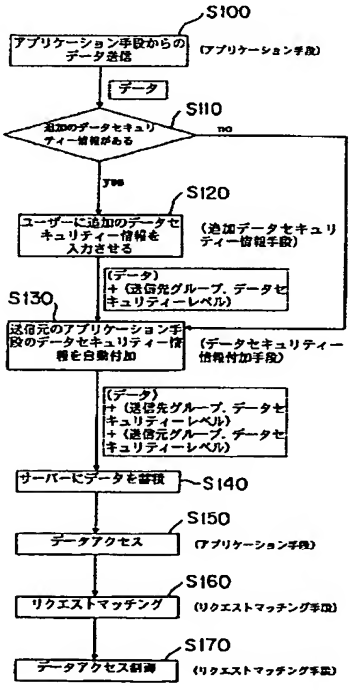
(21)出願番号　特願平10－72563

(22)出願日　平成10年(1998)３月20日

(71)出願人　000155469
株式会社野村総合研究所
東京都千代田区大手町二丁目２番１号
(72)発明者　斎　藤　倫　彦
神奈川県横浜市保土ケ谷区神戸町134番地
株式会社野村総合研究所内
(74)代理人　弁理士　佐藤　一雄　（外２名）

(54)【発明の名称】　データアクセス制御を行うデータ通信システム

(57)【要約】
【課題】　データアクセス制御を行うシステムとして全体として簡単な構成を有しており、維持管理が簡単であり、かつ、確実にデータの機密を保持できるデータ通信システムを提供する。
【解決手段】　複数のアプリケーション手段ＡＰと、データ通信ネットワーク２と、データのアクセス制御を行うデータアクセス制御システム３と、を有し、アプリケーション手段ＡＰは、データセキュリティーレベルをそれぞれ付与されており、データアクセス制御システム３は、データセキュリティー情報を付加するデータセキュリティー情報付加手段と、データを受信して蓄積するサーバーと、蓄積データにアクセスを試みたアプリケーション手段のデータセキュリティーレベルとアクセスを試みられたデータのデータセキュリティー情報についてリクエストマッチングを行うリクエストマッチング手段と、を備えるようにした。



【特許請求の範囲】
【請求項１】データ通信を行って所定のデータ処理を行う複数のアプリケーション手段と、データ通信を行うデータ通信ネットワークと、前記アプリケーション手段と前記データ通信ネットワーク間のインタフェースをなしてデータのアクセス制御を行うデータアクセス制御システムと、を有するデータ通信システムであって、
前記アプリケーション手段は、アクセスできるデータの機密の度合いに応じて定められたデータセキュリティーレベルをそれぞれ付与されており、
前記データアクセス制御システムは、送信データに送信元のアプリケーション手段のデータセキュリティーレベルをデータセキュリティー情報として付加して送信のために必要により前記データ通信ネットワークに渡すデータセキュリティー情報付加手段と、データを受信して蓄積するサーバーと、前記サーバーに蓄積されたデータにアクセスを試みたアプリケーション手段のデータセキュリティーレベルとアクセスを試みられたデータのデータセキュリティーレベルとを比較し、アクセスを試みたアプリケーション手段のデータセキュリティーレベルがアクセスを試みられたデータのデータセキュリティーレベル以上の場合にのみそのアプリケーション手段によるデータアクセスを許可するリクエストマッチング手段と、を有していることを特徴とするデータアクセス制御を行うデータ通信システム。
【請求項２】前記アプリケーション手段は、階層化された複数のデータセキュリティーレベルを内有するグループの少なくとも一つに属し、
前記データアクセス制御システムのデータセキュリティー情報付加手段は、送信データに送信元のアプリケーション手段のグループ及びそのデータセキュリティーレベルをデータセキュリティー情報として付加し、送信のために必要により前記データ通信ネットワークに渡し、
前記データアクセス制御システムのリクエストマッチング手段は、前記サーバーに蓄積されたデータにアクセスを試みたアプリケーション手段のグループ及びデータセキュリティーレベルとアクセスを試みられたデータのデータセキュリティー情報中のグループ及びデータセキュリティーレベルとを比較し、アクセスを試みたアプリケーション手段のグループがアクセスを試みられたデータのデータセキュリティー情報中のグループと同一であって、かつ、アクセスを試みたアプリケーション手段のデータセキュリティーレベルがアクセスを試みられたデータのデータセキュリティー情報中のデータセキュリティーレベル以上となる場合が少なくとも一つあるときにのみそのアプリケーション手段によるデータアクセスを許可するように構成されていることを特徴とする請求項１に記載のデータアクセス制御を行うデータ通信システム。
【請求項３】前記アプリケーション手段と前記データアクセス制御システムのいずれかは、データを送信するユーザーに、必要により任意のデータセキュリティーレベルあるいは任意のデータセキュリティーレベル及びグループを追加のデータセキュリティー情報として送信データに追加させる追加データセキュリティー情報手段を有していることを特徴とする請求項１または２に記載のデータアクセス制御を行うデータ通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データアクセス制御を行うデータ通信システムに係り、特に、データのアクセス制御をアプリケーション手段から切り離し、通信システムの基盤システムの一部として行うようにしたデータ通信システムに関する。
【０００２】なお、ここでデータのアクセスとは、データを取得できるようにすること、あるいはデータの内容を閲覧できることをいう。また、アプリケーション手段は、特定の目的のためのデータ処理をするソフトウェアプログラムによって制御された情報処理装置をいう。
【０００３】
【従来の技術】今日、情報通信技術の発達により、色々なデータセキュリティーレベルを有する多数のユーザーが共通のデータ通信ネットワークを使用してデータ通信を行っている。ここで、データセキュリティーレベルとは、アクセスできるデータの機密の度合いに応じて定められたものであり、ユーザーのデータに対するアクセス権限をいうものとする。
【０００４】従来のデータ通信では、共通のデータ通信ネットワークを通じて種々の機密の度合いを有するデータがやり取りされるので、データを所望の送信先以外のユーザーに傍受されたくない場合には様々な手段が講じられている。
【０００５】第一に、ユーザーが使用する情報処理装置で、データのアクセスを制御する方法がある。ユーザーが使用する情報処理装置は、ソフトウェアプログラムによって制御されており、上記方法は、上記ソフトウェアプログラムによってユーザーのデータアクセス権限を認証し、データのアクセス制御を行うものである。
【０００６】このユーザーの情報処理装置のソフトウェアプログラムによって個別にデータアクセス制御を行うものには、オペレーションシステムレベルでデータアクセス制御を行うものと、アプリケーション手段のレベルでデータ制御を行うものがある。これらいずれのレベルのデータアクセス制御も、ユーザーの情報処理装置ごとに個別にデータアクセス制御を行う点では変わりない。具体的には、ユーザーによるデータアクセスの要求があった場合には、その要求を受けた情報処理装置で、そのユーザーによるデータアクセスが予定の取決めによって許可されているかどうかを確認し、許可されている場合にのみデータアクセスを許可するようにしたものであ

る。

【０００７】第二に、特定の送信先のみがデータを受信できるようにした方法がある。これは、通信プロトコルによって特定の送信先と通信チャンネルを保持し、所望の送信先以外のユーザーによるデータ傍受を排除する方法である。オンライン通信等はその端的な一例である。なお、この場合も、受信する情報処理装置でユーザーがそのデータを受信可能か否かの確認をする部分がある点で、上述した個別の情報処理装置でユーザーによるデータアクセスを制御する方法を一部有している。

【０００８】第三に、データを暗号化する方法がある。これは、データを暗号化し、特定のユーザー以外は暗号化データを復号化できないようにしたものである。これによれば、たとえデータを傍受されたとしても、その内容を解読されないようにすることができる。データの暗号化の方法としては、例えば公開鍵秘密鍵方式がある。

【０００９】

【発明が解決しようとする課題】しかしながら、上記従来の通信データの機密保持の方法では、データの機密保持が不確実であったり、データの機密を保持するための作業が煩雑であったり、あるいは通信効率が低いという問題があった。

【００１０】最初の個別の情報処理装置でユーザーのデータのアクセス制御を行う方法の課題について説明する。ユーザーの個別の情報処理装置でデータのアクセス制御を行う方法によれば、空間的に多数の情報処理装置が分散配置された状態で、すべての情報処理装置においてデータの機密保持を完全に維持するのは困難であった。つまり、各情報処理装置にデータアクセス制御を行うソフトプログラムが存在するので、不正なユーザーによるソフトプログラムの改竄とデータアクセスの可能性があった。

【００１１】また、この方法では、データのアクセス制御機能を多数の情報処理装置のソフトウェアプログラム中に組み込まなければならないので、データ通信システムを構成すること自体に全体として膨大な作業を必要とし、改変が必要な場合にも膨大な作業を必要としていた。

【００１２】また、データ通信システムにおけるデータセキュリティー（データの機密保持）に対しては、個別にデータセキュリティーレベルを設定してデータアクセス制御を行うより、統一的なデータセキュリティーレベルの下で統一的なデータアクセス制御を行う方が好ましい。

【００１３】次に、通信プロトコルによって特定の送信先と通信チャンネルを保持し、それ以外のユーザーによるデータ傍受を排除する方法の課題について説明する。この方法によれば、データを送信する際に、送信先を指定する必要がある。しかし、送信先が多数ある場合には、すべての送信先を指定することになり、不便である。現実のデータ通信の場面では、一定のデータアクセス権限以上のすべてのユーザーは自由にアクセスできる条件でデータを送信したい場合が多い。この要求に対しては、上記従来の方法では、そのまま対応することができなかった。

【００１４】また、限定的な通信局間でのみ通信をする関係上データの通信効率の面からも好ましくない問題を有していた。

【００１５】また、この方法によっても、受信する情報処理装置でユーザーの認証を行わなければならない。このため、物理的空間的に分散した多数の情報処理装置で、データアクセス制御を行うプログラムが存在し、上記個別の情報処理装置でユーザーのデータアクセスを制御する方法と本質的に同じ課題を有する。

【００１６】次に、データの暗号化・復号化の方法の課題について説明する。データの暗号化・復号化の方法は、データを暗号化・復号化する必要があり、かつ、たとえば公開鍵秘密鍵方式では、各ユーザーが公開鍵を公表し、各自が秘密鍵を保持する。

【００１７】しかし、この方法では、例えば同一企業内のデータセキュリティーの目的のためには、システムがあまりにも複雑になりすぎる問題があった。現実のデータ通信の場面では、データ自体を暗号化することなく、データの閲覧を防止できればよい場合が多い。このため、このデータの暗号化・復号化の方法より簡単だが確実なデータアクセス制御の方法が求められていた。

【００１８】そこで、本発明の解決しようとする課題は、上記従来技術の問題点に鑑み、データアクセス制御を行うシステムとして全体として簡単な構成を有しており、維持管理が簡単であり、かつ、確実にデータの機密を保持できるデータ通信システムを提供することにある。

【００１９】

【課題を解決するための手段】本願請求項１に係るデータアクセス制御を行うデータ通信システムは、データ通信を行って所定のデータ処理を行う複数のアプリケーション手段と、データ通信を行うデータ通信ネットワークと、前記アプリケーション手段と前記データ通信ネットワーク間のインタフェースをなしてデータのアクセス制御を行うデータアクセス制御システムと、を有するデータ通信システムであって、前記アプリケーション手段は、アクセスできるデータの機密の度合いに応じて定められたデータセキュリティーレベルをそれぞれ付与されており、前記データアクセス制御システムは、送信データに送信元のアプリケーション手段のデータセキュリティーレベルをデータセキュリティー情報として付加して送信のために必要により前記データ通信ネットワークに渡すデータセキュリティー情報付加手段と、データを受信して蓄積するサーバーと、前記サーバーに蓄積されたデータにアクセスを試みたアプリケーション手段のデー

タセキュリティーレベルとアクセスを試みられたデータのデータセキュリティーレベルとを比較し、アクセスを試みたアプリケーション手段のデータセキュリティーレベルがアクセスを試みられたデータのデータセキュリティーレベル以上の場合にのみそのアプリケーション手段によるデータアクセスを許可するリクエストマッチング手段と、を有していることを特徴とするものである。

【００２０】本願請求項２に係るデータアクセス制御を行うデータ通信システムは、請求項１に記載のデータ通信システムにおいて、前記アプリケーション手段は、階層化された複数のデータセキュリティーレベルを内有するグループの少なくとも一つに属し、前記データアクセス制御システムのデータセキュリティー情報付加手段は、送信データに送信元のアプリケーション手段のグループ及びそのデータセキュリティーレベルをデータセキュリティー情報として付加し、送信のために必要により前記データ通信ネットワークに渡し、前記データアクセス制御システムのリクエストマッチング手段は、前記サーバーに蓄積されたデータにアクセスを試みたアプリケーション手段のグループ及びデータセキュリティーレベルとアクセスを試みられたデータのデータセキュリティー情報中のグループ及びデータセキュリティーレベルとを比較し、アクセスを試みたアプリケーション手段のグループがアクセスを試みられたデータのデータセキュリティー情報中のグループと同一であって、かつ、アクセスを試みたアプリケーション手段のデータセキュリティーレベルがアクセスを試みられたデータのデータセキュリティー情報中のデータセキュリティーレベル以上となる場合が少なくとも一つあるときにのみそのアプリケーション手段によるデータアクセスを許可するように構成されていることを特徴とするものである。

【００２１】本願請求項３に係るデータアクセス制御を行うデータ通信システムは、請求項１または２に記載のデータ通信システムにおいて、前記アプリケーション手段と前記データアクセス制御システムのいずれかは、データを送信するユーザーに、必要により任意のデータセキュリティーレベルあるいは任意のデータセキュリティーレベル及びグループを追加のデータセキュリティー情報として送信データに追加させる追加データセキュリティー情報手段を有していることを特徴とするものである。

【００２２】

【発明の実施の形態】以下に、本発明の実施の形態について願書に添付した図面を用いて説明する。

【００２３】図１は、本発明の一実施形態による「データアクセス制御を行うデータ通信システム」の構成を概念的に説明したものである。

【００２４】図１に示すように、本発明によるデータ通信システム１は、複数のアプリケーション手段ＡＰと、データ通信ネットワーク２と、アプリケーション手段ＡＰとデータ通信ネットワーク２とのインタフェースをなすデータアクセス制御システム３とからなる。

【００２５】上記アプリケーション手段ＡＰは、データ通信を行って特定の目的のためのデータ処理を行うものである。実体的には、アプリケーション手段ＡＰは、所定のデータ処理を行うようにソフトウェアプログラムによって制御された情報処理装置をいう。

【００２６】なお、本明細書で、後述するようにアプリケーション手段ＡＰに情報のアクセス権限たるデータセキュリティーレベルが付与されているという場合、あるいはアプリケーション手段ＡＰがその送信データに追加のデータセキュリティー情報を付加するという場合には、アプリケーション手段を使用するユーザーは固定されていると考え、ユーザーのデータセキュリティーレベルがアプリケーション手段ＡＰに付与されている、あるいは、ユーザーが送信データに追加のデータセキュリティー情報を付加することをいうものとする。すなわち、システム上、アプリケーション手段ＡＰはユーザーを含めた一体的な存在として取扱うのである。その場合、アプリケーション手段ＡＰに対するデータアクセスの許可あるいは不許可は、それを使用するユーザーへのデータアクセスの許可あるいは不許可と同一意味を有する。

【００２７】上記データ通信ネットワーク２は、データ通信を行うシステムである。データ通信ネットワーク２は公知の構成を有しているものでよく、実体的には、通信回線網、制御機、交換機等のハードウェアと、経路選定、交換等の通信を行うための制御を行うソフトウェアとからなる。

【００２８】上記データアクセス制御システム３は、本発明の特徴的なデータアクセス制御を行う部分である。データアクセス制御システム３は、上記データ通信ネットワーク２とアプリケーション手段ＡＰ間のインタフェースをなす。ここで、インタフェースをなすとは、以下の諸機能を果たすことをいう。

【００２９】①　アプリケーション手段ＡＰからの送信をデータ通信ネットワーク２に中継する。中継に際し、各アプリケーション手段ＡＰとデータ通信ネットワーク２のコマンドやレスポンスなどの論理的特性を一致させ、正常な接続のための処理を行う。

【００３０】②　アプリケーション手段ＡＰからの送信を中継する際に、後述するデータセキュリティー情報を送信データに付加する。

【００３１】③　送信されたデータを一時的に蓄積し、そのデータにアクセスするアプリケーション手段に対するデータアクセス制御、すなわち、データアクセスの許可と不許可の判定と制御を行う。

【００３２】本実施形態では、上述したインタフェースとデータアクセス制御の機能を果たすため、データアクセス制御システム３は、図１に示すように、複数のサーバーＳ１，Ｓ２，…，Ｓｎからなる。各サーバーＳ１，

S2，…，Snは物理的には、通信機能を有し、アクセス制御を行うためのデータ処理を行うことが可能な情報処理装置からなる。

【００３３】各サーバーS1，S2，…，Snには、複数のアプリケーション手段ＡＰがクライアント群として接続されている。一つのサーバーに接続するアプリケーション手段ＡＰ群が、共通の種類の情報を取扱う一つのグループを形成する。アプリケーション手段ＡＰがグループを形成するのは、グループの内外で情報の機密の度合いが相違するからである。グループの分かりやすい例としては、例えば、一企業内における総務部門、経理部門、人事部門などがある。これら各部門（各情報グループ）の同一部門内では、他部門に対してはかなり高度な機密性を有する情報も同部門の大部分のユーザーが共有することになる。すなわち、同一のデータでも、同一グループ内でやり取りする場合と他グループに対して送信する場合とでは、データの機密の度合いが異なるのである。

【００３４】また、同一グループ内でも、ユーザーによってアクセスすることができるデータの機密の度合いが相違する。この同一グループ内のデータアクセス権限（データセキュリティーレベル）の相違により、同一グループ内のデータアクセス制御が行われる。

【００３５】所定のユーザーすなわちアプリケーション手段ＡＰからの送信は、同一グループに対するものと、他グループに対するものとがある。

【００３６】同一グループに対する送信は、図１におけるアプリケーション手段ＡＰ1からの送信がこれに該当する。アプリケーション手段ＡＰ1から同一グループへのデータの送受信は、最初に送信データがアプリケーション手段ＡＰ1からその同一グループのサーバーS2に送られてそこに蓄積され、同一グループの他のアプリケーション手段ＡＰのアクセスによって、データが受け渡されることで実現される。

【００３７】この場合、アプリケーション手段ＡＰ1からサーバーS2にデータが送られてそこに蓄積され時に、そのデータにアクセス可能なアプリケーション手段ＡＰについて規定する情報（後述するデータセキュリティー情報）が付与される。後に、当該データに他のアプリケーション手段ＡＰからデータアクセスの要求があった場合に、そのデータセキュリティー情報が参照され、データに付与されたデータセキュリティー情報より高度なデータアクセス権限を有するアプリケーション手段ＡＰによるデータアクセスのみが許可される。

【００３８】次に、他のグループに対するデータの送受信について説明する。図１におけるアプリケーション手段ＡＰ2からの送信がこれに該当する。アプリケーション手段ＡＰ2から他のグループへのデータの送受信は、最初に送信データがアプリケーション手段ＡＰ2の接続サーバーS1に送られることから始まる。サーバーS1は、送信元のアプリケーション手段ＡＰ2のデータセキュリティレベル情報および追加のデータセキュリティー情報を付加し、データ通信ネットワーク２にデータを渡し、データ通信ネットワーク２の機能によって送信先グループのサーバーSnにデータを送信する。なおこの場合、送信先のサーバーを特定せず、データ通信ネットワーク２に接続されたすべてのサーバーに送信するようにしてもよい（ブロードキャスト通信）。

【００３９】サーバーSnは、サーバーS1によって転送されたデータを受信し、それを蓄積する。このサーバーSnに接続されたアプリケーション手段ＡＰは、定期的にあるいはサーバーからデータ受信の知らせを受けてデータのアクセスを試みる。アプリケーション手段ＡＰからデータのアクセス要求を受けたサーバーSnは、アクセスを試みたアプリケーション手段ＡＰのデータセキュリティーレベルとアクセスを試みられたデータのデータセキュリティー情報とを比較し、アクセスを試みたアプリケーション手段ＡＰのグループがデータセキュリティー情報のグループと同一であり、かつ、アクセスを試みたアプリケーション手段ＡＰのデータセキュリティーレベルがアクセスを試みられたデータのデータセキュリティーレベル以上である場合にのみデータアクセスを許可するのである。

【００４０】以上により、送信元のアプリケーション手段ＡＰ2が指定したグループの所定のデータアクセス権限以上のアプリケーション手段ＡＰのみがそのデータにアクセスすることができる。

【００４１】なお、図１の例ではデータ通信ネットワーク２のサーバーは、同一の情報種類を共有するグループごとに一つ存在する構成となっていたが、サーバーは、複数存在する必要はなく、データアクセス制御を統一的に行う全システムにおいて単一のサーバーとしてもよい。また、複数のグループが同一のサーバーを共有することもできる。さらに、データ通信ネットワーク２の全体の通信制御を行っている情報処理装置がその制御を行ってもよい。

【００４２】次に、上記データアクセス制御の詳細について図２を用いて説明する。本発明によるデータアクセス制御を行うデータ通信システムにおいて、アプリケーション手段は、それぞれ自らが取扱えるデータの機密の度合いを規定したデータセキュリティーレベルを付与されている。

【００４３】なお、アプリケーション手段は、階層化された複数のデータセキュリティーレベルを内有するグループの少なくとも一つに属するものとする。

【００４４】データアクセス制御システムは、データセキュリティー情報付加手段と、受信したデータを蓄積するサーバーと、リクエストマッチング手段と、を有している。

【００４５】データセキュリティー情報付加手段は、送

信データに送信元のアプリケーション手段のデータセキュリティーレベルをデータセキュリティー情報として付加し、必要によりデータ通信ネットワークに渡す処理を行う手段である。

【００４６】リクエストマッチング手段は、前記サーバーに蓄積されたデータにアクセスを試みたアプリケーション手段のデータセキュリティーレベルとアクセスを試みられたデータのデータセキュリティー情報とを比較し、アクセスを試みたアプリケーション手段のグループとアクセスを試みられたデータのデータセキュリティー情報中のグループと同一であって、かつ、アクセスを試みたアプリケーション手段のデータセキュリティーレベルがアクセスを試みられたデータのデータセキュリティー情報中のデータセキュリティーレベル以上となる場合が少なくとも一つあるときにのみそのアプリケーション手段によるデータアクセスを許可する手段である。

【００４７】また、以下の説明では、データを送信するユーザーに、必要により任意のデータセキュリティーレベルあるいは任意のデータセキュリティーレベル及びグループを追加のデータセキュリティー情報として送信データに追加させる追加データセキュリティー情報手段がアプリケーション手段あるいはデータアクセス制御システムのいずれかに設けられているものとする。

【００４８】以上の本発明のデータ通信システムを構成する各手段は、実体的には、上述したような処理を行うソフトウェアプログラムによって制御された情報処理装置である。これら情報処理装置は、その処理を行う限り、物理的な配置構成に依存しない。

【００４９】次に、図２に沿って上記各手段間の処理の関連、流れについて説明する。図２において、各ブロックは処理の内容を示し、各ブロックの出力の矢印の側に破線で囲って示したものは出力されるもの内容を示し、各ブロックの側にかっこで囲って示したものはその処理を行う本データ通信システムの構成手段である。

【００５０】図２に示すように、最初にあるアプリケーション手段（これを送信元アプリケーション手段ということにする）からデータを送信するものとする（ステップＳ１００）。データの送信要求は、データアクセス制御システム（物理的にはその所定のサーバー）に送られる。

【００５１】次に、送信元アプリケーション手段あるいはデータアクセス制御システムのいずれかにより、追加のデータセキュリティー情報の有無が確認される（ステップＳ１１０）。

【００５２】追加のデータセキュリティー情報が有れば、追加データセキュリティー情報手段を介して、送信をしようとするユーザーによりそのデータを受信可能な送信先グループとそのグループにおけるデータセキュリティーレベルが指定される。（ステップＳ１２０）。

【００５３】上記追加のデータセキュリティー情報を付加した送信データは、データアクセス制御システムのデータセキュリティー情報付加手段に送られる。一方、上記ステップＳ１１０で追加データセキュリティー情報が無いと確認された送信データもそのままデータアクセス制御システムのデータセキュリティー情報付加手段に送られる。ここで、データセキュリティー情報付加手段により、送信データにデータ送信元のアプリケーション手段のグループとデータセキュリティーレベルが付加される（ステップＳ１３０）。

【００５４】上記ステップＳ１３０の処理により、送信データに送信元アプリケーション手段のグループとデータセキュリティーレベル、および必要により送信先アプリケーション手段のグループとそのデータセキュリティーレベルの情報（データセキュリティー情報）が付加される。このデータセキュリティー情報を付加したものは、データアクセス制御システムの所定のサーバーに送信され、そこに蓄積される（ステップＳ１４０）。

【００５５】このサーバーに蓄積されたデータには、定期的にあるいはデータ受信の知らせを受けてアプリケーション手段がアクセスを試みる（ステップＳ１５０）。

【００５６】データアクセスの要求があった場合には、データアクセス制御システムのリクエストマッチング手段により、データのデータセキュリティー情報とアクセスしようとするアプリケーション手段のデータセキュリティーレベルとが比較される（ステップＳ１６０）。

【００５７】この結果、アクセスを試みたアプリケーション手段のグループがアクセスを試みられたデータのデータセキュリティー情報中のグループと同一であり、かつ、アクセスを試みたアプリケーション手段のデータセキュリティーレベルがアクセスを試みられたデータのデータセキュリティー情報中のデータセキュリティーレベル以上の場合にのみデータのアクセスを許可する（ステップＳ１７０）。

【００５８】上記リクエストマッチングとデータアクセス制御を具体例と図３を用いて説明する。

【００５９】図３は、Ａ，Ｂ，Ｃという三人のユーザーがそれぞれ別々のグループに属し、各グループにおいて別々のデータセキュリティーレベルを有している場合において、ユーザーＢからデータＤが送信された場合の各ユーザーに対するデータアクセス制御を説明したものである。

【００６０】図３の例では、３つの同種情報を取扱うグループＭ，Ｎ，Ｐが存在する。分かりやすさのために、仮にグループＭは総務部門、グループＮは経理部門、グループＰは人事部門とする。グループＭ，Ｎ，Ｐは、社内共通の階層化されたデータセキュリティーレベル１，２，…，Ｎを内有しているとする。

【００６１】ユーザーＡは、グループＭ（例えば総務部門）の責任者であり、グループＭ内では最高のデータセキュリティーレベルＮを有し、グループＭ内のデータな

ら如何なるデータにもアクセスできるものとする。グループP（人事部門）については、ユーザーAは、ある程度の機密性を有するデータにアクセスでき、グループP内でデータセキュリティーレベル2を有している。しかし、グループN（経理部門）については、ユーザーAは、如何なるデータにもアクセスできず、データセキュリティーレベルを有していないとする。

【0062】ユーザーBは、グループN（（経理部門）の部員とする。ユーザーBは、その職務上グループN（（経理部門）内でデータセキュリティーレベル2を有しているとする。ユーザーBは、グループM（総務部門）にデータセキュリティーレベル1を有している。

【0063】ユーザーCは、グループP（人事部門）の責任者であり、グループP内では最高のデータセキュリティーレベルNを有し、グループP内のデータ（人事データ）なら如何なるデータにもアクセスできるものとする。グループN（経理部門）については、ユーザーCは、ある程度の機密性を有するデータにアクセスでき、グループN内でデータセキュリティーレベル2を有している。一方、グループM（総務部門）については、ユーザーCは、如何なるデータにもアクセスできず、データセキュリティーレベルを有していないとする。

【0064】上記ユーザーのグループとデータセキュリティーレベルは、図3の下の表の左列の各欄に記載され、リクエストマッチング時に判断の基準となる。

【0065】今、ユーザーBがデータDを送信したとする。データDには、データアクセス制御システムのデータセキュリティー情報付加手段により、送信元のデータセキュリティー情報として、グループN．データセキュリティーレベル2が自動的に付加される。

【0066】さらに、ユーザーBが、グループMとPの責任者すなわちデータセキュリティーレベルN以上のユーザーがアクセス可能なように、追加データセキュリティー情報手段により追加のデータセキュリティー情報を付加したとする。

【0067】上記データDのデータセキュリティー情報は、図3の中段に記載されたようになる。すなわち、（グループM．データセキュリティーレベルN）＋（グループN．データセキュリティーレベル2）＋（グループP．データセキュリティーレベルN）となる。

【0068】このデータDにユーザーA，B，Cがそれぞれアクセスを試みたとすると、そのリクエストマッチングの結果は図3の下部の表のようになる。表中の○は、リクエストがアクセスを許可する条件をマッチしている場合を示す。他方、表中の×は、リクエストがアクセスを許可する条件をマッチしていない場合を示す。

【0069】簡単なために、ユーザーAの場合についてのみ説明する。ユーザーAは、（グループM．データセキュリティーレベルN）というデータセキュリティーレベルと、（グループP．データセキュリティーレベル2）というデータセキュリティーレベルを有している。このユーザーAのデータセキュリティーレベルとデータDのデータセキュリティー情報について、同一グループのデータセキュリティーレベルを比較すると以下のようになる（データセキュリティーレベルを単にレベルと略記する）。

ユーザーA：
（グループM．レベルN）　＝（グループM．レベルN）→　マッチ
（グループN．レベル　無）＜（グループN．レベル2）→　不マッチ
（グループP．レベル2）　＜（グループP．レベルN）→　不マッチ

リクエストがマッチする場合が一つでもあれば、そのユーザーA（アプリケーション手段）によるデータアクセスが許可され、リクエストマッチする場合が皆無な場合は、データアクセスが許可されない。

【0070】なお、本願請求項中、アプリケーション手段のデータセキュリティーレベルがデータセキュリティー情報中のデータセキュリティーレベル以上とは、上述したように、アプリケーション手段のデータセキュリティーレベルがデータセキュリティー情報中のデータセキュリティーレベルに比してデータアクセス権限上高い位置にある状態をいうものとする。

【0071】

【発明の効果】このように、本発明による「データアクセス制御を行うデータ通信システム」によれば、データのアクセス制御は、そのデータアクセス制御システムが、アプリケーション手段から切り離され、集中的に管理可能になる。データアクセス制御システムがアプリケーション手段が切り離されることにより、不正なユーザーによる改竄を防止でき、データの漏洩の可能性を低くすることができる。また、データアクセス制御システムが集中的に管理可能になることにより、システムが容易に監視でき、仮に不正な改竄やデータアクセスがあった場合にも発見が容易になる。

【0072】また、本発明のシステムによれば、データそのものを暗号化する必要が無く、必要な場合には、データの内容をそのまま把握でき、便利である。

【0073】また、一定のデータアクセス権限以上のユーザーから誰でもデータアクセスできるという設定ができ、実際の使用要求に即して高い効率で情報のやり取りを行うこともできる。

【0074】データアクセスの管理の面からも、統一的なデータセキュリティーレベルで全体のデータアクセス制御が可能であり、簡素な情報管理体系の構築が可能になる。

【0075】まち、本発明のデータ通信システムによれば、データのアクセス制御を行う装置とソフトウェアが

アプリケーション手段から独立しているので、システム構築時のデータアクセス制御のためのプログラミングの労力が大幅に軽減され、その改変があった場合の労力も大幅に軽減される。

【００７６】最後に、本発明のデータ通信システムによれば、送信データは最初にすべてのグループに送信され、それ以降のデータのアクセスが制御される。このことにより、本発明のデータ通信システムでは、ブロードキャスト方式による通信が可能になり、通信効率の面で改善を図ることができる。

【図面の簡単な説明】

【図１】本発明の「データアクセス制御を行うデータ通信システム」システム構成を概念的に示した図。

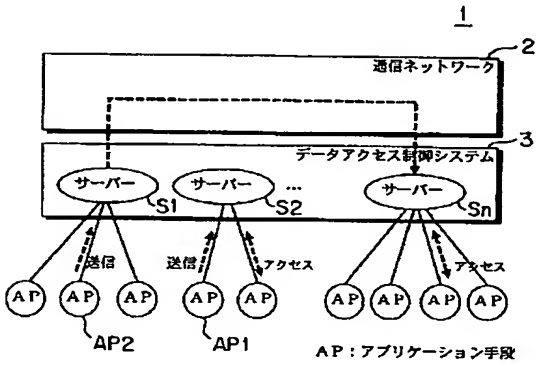
【図２】本発明の「データアクセス制御を行うデータ通信システム」による処理の流れを示したフローチャート。

【図３】本発明の「データアクセス制御を行うデータ通信システム」によるリクエストマッチングを具体例を用いて説明した図。

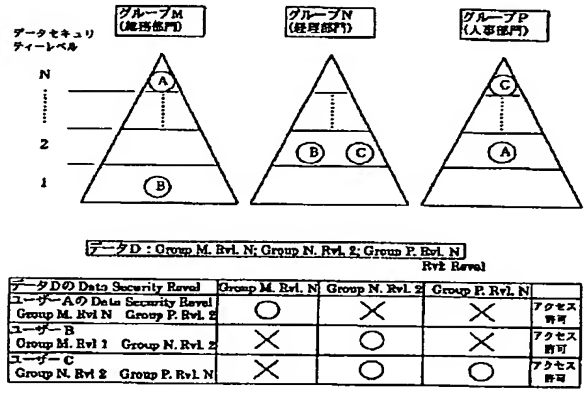
【符号の説明】

１　データ通信システム
２　データ通信ネットワーク
３　データアクセス制御システム
ＡＰ　アプリケーション手段
Ｓ　サーバー

【図１】

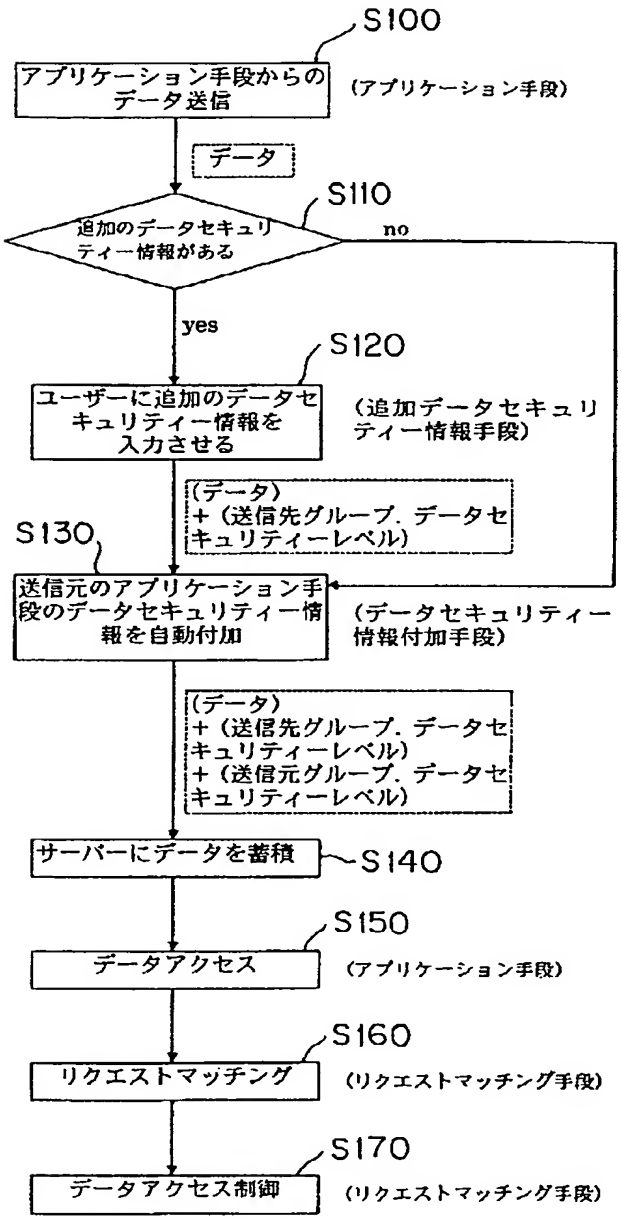


【図３】



データDの Data Security Reval	Group M. Rvl. N	Group N. Rvl. 2	Group P. Rvl. N	
ユーザーAの Data Security Reval Group M. Rvl N　Group P. Rvl. 2	○	×	×	アクセス許可
ユーザーB Group M. Rvl 1　Group N. Rvl. 2	×	○	×	アクセス許可
ユーザーC Group N. Rvl 2　Group P. Rvl. N	×	○	○	アクセス許可

【図2】



フロントページの続き

(51)Int.Cl.⁶	識別記号	FI	
H04L 9/36		H04L 9/00	685